ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Investigation on Privacy Issue of Crypto-Currency Mining in India

Kiran Kumar Kaki

School of Computer Science and Engineering, Lovely Professional University, Phagwara , Punjab, India

Kiran.kaki@lpu.co.in

Ankita sharma

Assistant Professor, CSE Lovely Professional University

Jalandhar , Punjab

ankita.25080@lpu.co.in

Abstract

Bitcoin is a prevalent cryptographic money records theexchanges in dispersed affix just display the data called block-chain.In 2009, Bit-coin prudence hasgrow at extremely large rate, and current the value is 170 billionsdollars. This growth in the market approximation of Bit-coin propels for to abuse fault for profit, and scientists to find new weakness in the architecture , propose solutionsand up-coming patterns. In this paper , we formulate the privacy issue in the bit-coin mining and illegal using bit coin in India with global market . This provides the future direction to reader.

Introduction

Indians began promoting their money in Bit-coin. This hike set some technically knowledgeable residents of the India to buy Bit-coins just as achieve something with the block-chain convention in India itself. The Satoshi imagined Bit-coin ,India likely could be the leading nation to dig in its believability as another money related framework. Consistently, we have been organize crypto-currency indeveloping a quick pace. There is nobody who comprehends Indian buyers superior to local organizations. Nation like India, where all esteem each thing through its money related value, the definite short approach to beat money and make money [1]. A crypto trade and

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

wallet would permit a huge number of residents of the India to turn out to be a piece of the crypto economy will be an extraordinary jump for the whole block-chain network.

Eight year ago , Visa, MasterCard and PayPal, which together make up over 97% of the worldwide market for installment administrations, slice off subsidizing to Wikileaks[2]. In this paper, we explore the data into two sections : section one explore the global crypto currency market with Indian crypto currency market. Section two describes the privacy problems in bit-coin.

2. Related Work

Pannu[3], this paper discuss greatlyhandle the security bitcoin issues . Few are twofold pay out, Finney assault, animal power assault, vector 76, Goldfinger. These assaults has a few arrangements such as Conjoin, Coinshuffle, xim, esteem shuffle, dandelion and so on. They basically focus on the privacy .ShailakJani[4], what is the crypto currency in india and global market . Karan Veer Singh[5] , this paper tell the the probability of the future currency and analyze the bit-coin in India .Mauro[6]we condense the essential open troubles and propose headings for future research towards provisioning stringent security and assurance systems for Bitcoin.

3 Results and Discussions

This segment divided into two subsections giving outcomes that were gotten from the diverse research papers. Firstly , we identify the globally landscape crypto currency with Indian

landscape. In second section describe security problems in bit-coins

3.1 Overview of Studies :

An increase in the frequency of the Bit coin attracted the researches to start working in this field so the publication increasein 2010 to 2019 .According to the report[5] , bit coin rises globally from Jan 2016 to October 2019

The Global Aspect:

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

In 18 March,2018 there are 1664 Crypto currencies accessible and exchanged around 9423 trades. The market economy valuefor all digital forms of money is $275,797,435,872 for example $335 Billions. and 22-hour worth was $ 18,207,953,778 i.e.$18 Billions . Fig 1. shows growth in digital currency market.

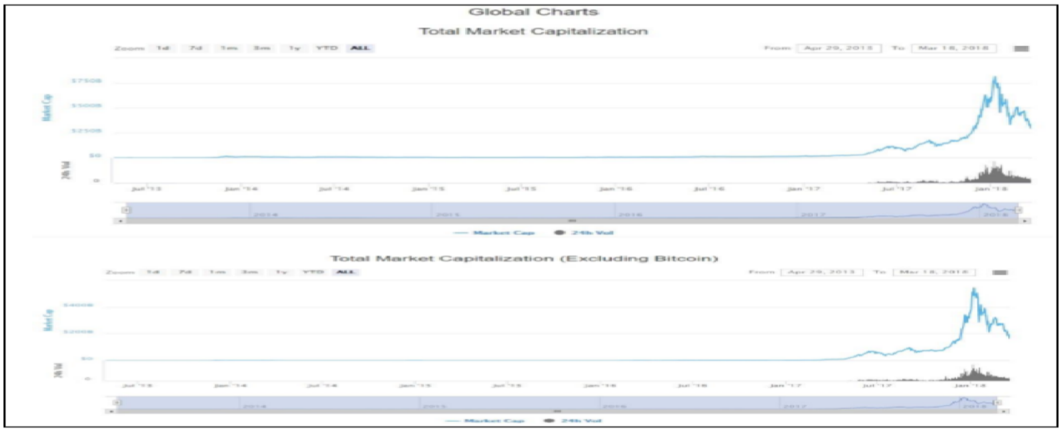

Fig: 1 Ratio of Global market

The Bit coin has most extreme predominance ,digital currency showcase with around 55% piece of the pie and market economy of $152.2 Billions (Rs 10.25 Trillion). The market value is $8254.9 i.e Rs 5,35,867. Different digital money forms barring bit coins is alluded all in all as bit coins, it incorporates other 1450 monetary standards that are exchanged. Some of crypto currency is bit coin price is $ 92,25 US and market cap is $142.2 B

According to the report [6],India is 4th out of top 10 countries. In India , people start doing mining in illegal manner, i.e 10 out 5 people is doing illegal mining.

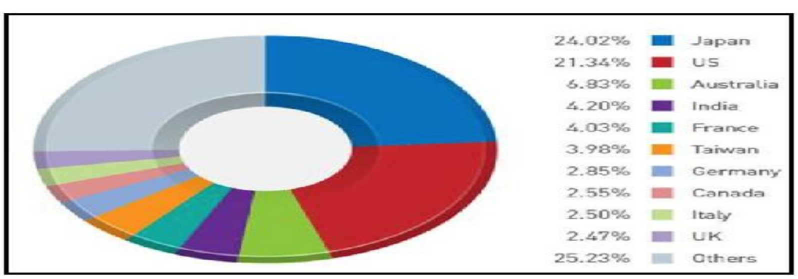

Fig 2: Country wise distribution of BitCoin

Indian Landscape:

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

The population of India is more than 1 billion in number. That is something of a financial renaissance over the most recent years. The degree of nation's development of the IMF is considered it quickest developing rising wealth. In excess of 40% of the nation's populace resembletelecoms and internet providers. This article takes a gander at the condition of the Indian digital currency showcase.

Expanding exchanging volumes and Bit coin exercises by huge edges are the underlying effect expected after the sanctioning of Bit coin in India. Authorization is probably going to empower According to Bit-coin new report, companies worries about the security and dangers starts when Bit coin use, in the end, move in the direction of the improvement of its foundation. Authorization improve in killing fears throughout its constant for normal Indian purchaser. Though, a few reports of Bit-coin exchanging proportionate to illegal tax avoidance that engenders the financing of psychological militant outfits. So as to get a murmur of help from these feelings of anxiety, Bit coin new businesses in India are executing numerous security checks. Fig 3 shows the illegal bit coins in India increase from 2 M to 5 M in 2019 .

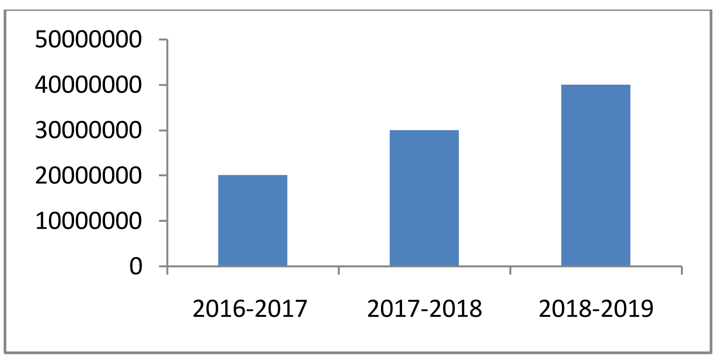

Fig 3: Increasing Number of bit-coin Mining in India

3.2 Privacy Problem in Bit-Coin

There are many security issue in the bit-coin .Table 1 describe the issue and risk factor of that issue . These issue are categorize into 7 categories and mapping with different research studies.

Table 1:Comparsions of security issues

Attack	Definition	Targets	Effects	Possible
Double spending or race attack[9]	Use the same bit-coin in different	Seller and merchant	Loss of product by seller , no	Creating users in networks ,

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

	transitions		honest users , block chain frocks	double alert among peer
Finney attack[10]	unscrupulous digger communicates a pre-dug obstruct with the end goal of twofold spending when it gets item from a dealer	Seller and merchant	encourages twofold spending	hang tight for multiple-confirm for exchanges
Brute-force attack [11]	secretly block-chain mining , perform fork to twofold spending	Seller and merchant	encourages twofold spending	Creating users in networks
1-configration attack [12]	encourages twofold spending	Bit-coin exchange service	encourages twofold spending	Creating users in networks
Gold finger[13]	Control is more than 50% hash rate	Miner of Bit-coin network	Create the race condition and working alone such as DoS	Creating users in networks
Selfish Mining [14]	Feature to drive an bit-coin forking	Trustworthy miner	Create the race condition and trustworthy miner is less than 50 %	Time based techniques
Block withholding[15]	Pool of the miner	Mining pools for honest user	Waste resource of fellow	Trusted miner pool
DDoS [16]	Cheater use the	Users , miners	Effects the	Machine learning

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

	network resources		network and services	

4. Conclusion

Bit-coin has quite recently shown a notable propelled money in the market. In any case, the praise of Bit-coin has destroyed in adversaries to use Bitcoin sort out for their egocentric aims and well-being. Today we have around 1250 particular computerized monetary standards, all things considered, out of which many are a continuous preface to the market. From all these financial structures, the momentous universality and high market capital of bitcoins make it appealing for adversaries to dispatch distinctive security threats. According to survey, in spite of the way that the advancement of the Bitcoin shows with check of-work and accord to verify the customer exercises are basically the solid features in Bitcoin, these transforming into a point of control for computerized criminals. Starting from group sniffing to the twofold spending, the Bitcoin is dreaded with various attacks. In spite of the way that composing gives game plans against relatively few of these attacks, the lively and convincing security game plans that can ensure suitable working of Bitcoin later on are up 'til now absent.The passed on thought of Bitcoinhas been lead thebreakdown in the insurance and anonymity necessities of the customers.In this paper we survey the illegal activities done in india through bitcoin and global data . Then we provide the issue in the bitcoin . The future scope is to find the tools flaws so that , we can find the culprit easily.

Reference :

[1]Available on :htttp://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20

on%20cryptocurrencies%20and%20blockchain.pdf

[2]Available On:https://www.theguardian.com/books/2019/jun/26/the-white-paper-satoshi-nakamoto-review

[3]Parmeet Singh Pannu ," Review on Security Problems of Bitcoin" 2019 .Springer Nature Switzerland AG 2020 A. P. Pandian et al. (Eds.): ICCBI 2018, LNDECT 31, pp. 180–184, 2020.

[4]ShailakJani, "The Growth of Crypto currency in India: Its Challenges & Potential Impacts on Legislation" -2018 ,Rersearch gate DOI: 10.13140/RG.2.2.14220.36486

[5]Arvindkumar Sigh, 2018 "CRYPTOCURRENCY IN INDIA - ITS EFFECT AND FUTURE ON ECONOMY WITH SPECIAL REFERENCE TO BITCOIN"..Journal of Advance Management Research, ISSN: 2393-9664 (JAMR)

[6]Mauro Conti, 2017 "A Survey on Security and Privacy Issues of Bitcoin" - arXiv:1706.00916v3 [cs.CR]

[7]Available on link: " https://www.statista.com/statistics/326707/bitcoin-price-index/"

[8]Available on link :"https://www.trendmicro.co.in/cloud-content/apac/images/pr/bitcoin.png"

[9] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in Proceedings of the 2012 ACM Conference on Computer and Communications Security, ser. CCS '12. New York, NY, USA: ACM, 2012, pp. 906–917.

[10] H. Finney, "Best practice for fast transaction acceptancehow high is the risk?" Available: https://bitcointalk.org/index.php?topic=3441. msg48384#msg48384, 2011.

[11] J. Heusser, "Sat solvingan alternative to brute force bitcoin mining," Available: https://jheusser.github.io/2013/02/03/satcoin.html, 2013.

[12] Vector67, "Fake bitcoins?" Available: https://bitcointalk.org/index. php?topic=36788.msg463391#msg463391, 2011. [58]

[13] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," 2013

[14] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Financial Cryptography and Data Security: 18th International Conference. Springer Berlin Heidelberg, 2014, pp. 436– 454.

[15] . Haber and W. S. Stornetta, "How to time-stamp a digital document," vol. 3, no. 2, 1991, pp. 99–111.

[16]Vasek, M., Thornton, M., Moore, T.: Empirical Analysis of Denial of Service Attacks in the Bitcoin Ecosystem (2014

